Apparatus and method for safeguarding electronic equipment from theft

Technical field of the invention

The invention relates to an apparatus and a method for preventing electronic equipment from theft.

Background of the invention

Current industrial as well as governmental and private investments in computerised equipment and electronic devices grow rapidly and these investments form property of considerable value to the owners. However, this valuable property also attracts people to commit criminal acts and in illegal ways get in possession of items belonging to others.

Not only the so-called hardware, i.e. interconnected electronic circuits with processing capacity, memories and displays, but also and perhaps even more vulnerable may be so-called software and content of various memory locations of, or in association with, the electronic devices. Occurrence? of sensitive data or material stored in a memory location of e.g. a laptop computer in wrong hands may have severe consequences to any company, organisation or enterprise as well as to a private person if content stored in memory locations of the computer is made public, for whatever reason.

Several mechanical means for prevention of computer thefts are offered on the market, especially for preventing people from stealing stationary desktop computers in offices. Those means may be for example metallic safety lockers or wires, which physically restrict people from opening or carrying the computer or its parts with them. Such physical means mostly are relatively expensive, cumbersome to install and not at all flexible. However, for mobile equipment like for instance portable

laptop computers, even less practical theft-preventing means are offered on the market, such as various attention attracting sirens and alarms. Most prior art safeguarding arrangements are software encryption systems, which for data protective reasons may be very useful although the electronic components do not lose their value after theft from the legitimate owner.

The UK patent application GB 2 304 810 A discloses a security arrangement with sensors detecting light levels inside of a personal computer housing or motion of the personal computer. Furthermore, the arrangement inside the computer consists of a dye capsule, which is intended to rupture and spray its content outwardly upon reception of an electrical signal. This signal is sent from an alarm output control when the personal computer is considered stolen. It is of course difficult to distinguish usual "every day" handling of the personal computer in reliable manners from unauthorised handling after the computer has been stolen. A clear disadvantage of an implemented security arrangement of that kind is the risk of numerous false alarms leading to strongly decreased acceptance of the arrangement.

The international patent application WO 97/03397 discloses a method and an arrangement for deterring computer-thefts by means of a protective device using detection with external sensors. Sensing is performed either by using a thin film with an electrically conductive film, or wall anchor plates mounted on a wall of the room in which the computer is used. It can also be performed by means of an external sensor disposed as an insert between the underside of the computer and the table surface on which the computer stands. However, a solution with a thin film conductive sensor suffers from the drawback, that the film will be destroyed each time the computer casing is opened, even when the casing is opened for normal service actions or for maintenance. This makes this method and arrangement less convenient as it requires restoration of the conductive thin film after having opened the computer casing in order to reach the original functional state again. A restoration of this kind is costly due to manual work required by professionals every time the computer casing has been opened.

Summary of the invention

An object of the present invention is to overcome the aforementioned drawbacks concerning prior art technology in connection with stationary and portable computers as well as with electronic devices and circuitry in general.

This object of the invention is accomplished by means of an apparatus for safeguarding electronic equipment, such as components in a computer, provided in a housing, comprising a monitoring internal sensor arrangement in connection with a control means, which is fed with measurement data to monitor whether the housing is closed or not,

characterised by

at least one energy provider, such as an internal or external power source;

voltage generating means, driven by power from the energy provider and controlled by the control means;

storage means, including a capacitor arrangement charged by the voltage generating means;

switching means, in connection with the storage means being adapted to be controlled by the control means; and

relayed connections between components of the the electronic equipment and the switching means, particularly chosen to get the electronic equipment irreversibly out of order when initiated by the control means in response to unauthorised opening of the housing.

A housing sensor means would be convenient, sensing if the housing is unauthorised opened, whereby the housing sensor means is adapted to send a warning signal to the control means, preferably a micro-controller, when sensing unauthorised opening. In another embodiment, a conceivable solution would be to use electronic equipment sensing means sensing unauthorised disconnection of at least one component in the electronic equipment, whereby the electronic equipment is adapted to

send an indication to the control means for activation of a destructive activation when detecting unauthorised disconnection.

The apparatus moreover comprises identification means, identifying a user and possibly authorising the user after comparison with a register, whereby the electronic equipment could be unlocked. Said identification means either comprises a so-called smart card reading means, operating with physical contacting or without physical contacting and/or a PIN-code reading means and/or any other human feature recognising means, such as a fingerprint and/or iris recogniser.

In order to guarantee provision of energy for running the safeguarding apparatus, an autonomous power supplying means such as a battery, preferably a rechargeable battery arrangement, may be provided, which is supplying the apparatus and its parts with the sufficient electric power after having been disconnected from a mains power outlet.

Suitably, said destruction means generates a pulse of high voltage and/or current, which is lead through the electronic circuitry, whereby essential components within the circuitry are irreversibly set out of order. Else, said destruction means could generate a destructive injection, preferably of a highly conductive, gluing and/or corroding chemical fluid, which is distributed over vulnerable and essential electronic components, whereby the components are irreversibly set out of order.

For enhanced flexibility, remote control means could be useful, by which remote signals from a remote control station can be received, and whereby actions can be taken by the safeguarding apparatus in response to sent remote signals.

Furthermore, prior art is afflicted with problems that are solved by a method for safeguarding electronic equipment, which electronic equipment is placed and protected in a housing. The housing comprises monitoring means, such as an internal sensor arrangement, to monitor whether the housing in closed or not and/or whether an authorised person operates the electronic equipment. The method is characterised

by connecting and controlling the destruction initiation means by the monitoring means and providing at least one destruction means in the electronic equipment, which means has been particularly chosen to set the electronic equipment irreversibly of order when initiated by a destruction initiation means, such as a controlling micro-controller.

Owing to the present invention as here described, a novel approach is presented that offers the market a convenient and cheap apparatus and a method inhibiting incentives for stealing computer-related devices. The present invention has the advantage that the trade-in value of electronic devices, possibly removed from stolen computers is diminished due to the irreversible damage caused to the devices. It also constitutes a more flexible way of safeguarding electronic equipment, without limiting the mobility of the device, such as a stationary or portable computer.

Brief description of the drawings

The above and further features, advantages and benefits of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters and figures refer to like parts throughout, and in which:

Fig 1 shows a schematic overview of comprised units in a first embodiment of the safeguarding apparatus according to the present invention,

Fig 2 is a flow chart illustrating the sequence of activation, sensing, destruction and indication of operational states of the apparatus and the method here described.

Detailed description

The following description is of the best mode presently contemplated for practising the invention. The description is not to be taken in a limiting sense, but is made merely for the purpose of describing the general principles of the invention. The scope of the invention should be ascertained with reference to the issued claims.

With reference to Fig 1, a block diagram is shown of a first embodiment of the present invention for safeguarding electronic equipment like for instance a stationary or a portable computer. The main functional units of the apparatus according to the invention are mounted on a standard-sized slot card, preferably a so-called PCI-card adapted to be connectable to a corresponding PCI-slot within the computer casing, which is a slot format provided in most personal computers of today. Normally, the motherboard of a personal computer has a bi-directional connection 301 directly to an external power source 300 via a transformer (not shown here). According to this first embodiment, the external power source 300 is also connected via a transformer to the motherboard of the personal computer, but via a destruction means 200. There may also be direct connection between an input/output 130 of the micro-controller 130 and the external power source connection 301, but this is optional. The destruction means 200 is provided on the PCI-card, and the destruction means 200 comprises a number of units, each of which has a certain functionality and is able to communicate bi-directionally with a micro-controller 100 via one of its inputs/outputs 120. The micro-controller 100 is in control of each action performed by the apparatus according to the invention including power management of the computer. The units of the destruction means 200 are the internal power management unit 205, a battery 210, preferably but not necessarily rechargeable, a voltage generating means 215, a capacitor arrangement 220, preferably including a plurality of capacitors connected in parallel, and finally a target component switch 225. Each one of the units of the destruction means 200 is connected to the micro-controller via inputs/outputs 206, 211, 216, 221 and 226 respectively.

Moreover, the micro-controller 100 communicates with a sensor means 400 via another of its inputs/outputs 140. The sensor means 400 is also mounted on the PCI-card, alternatively connected to it but attached in another position within the computer casing, and includes at least two main units. These main units are on one hand an IR-unit (infrared unit) 410 with an input/output 411 and on the other hand a reflective layer 430 attached to the inside of the casing of the personal computer. The

reflective layer 430 is preferably an adhesive, thin plastic film having stripes or another similar patterns or texture on it, with significant differences in contrast between its fields. Checkers as well as waved patterns are both conceivable for use in other embodiments of the present invention. The IR-unit 410 is mounted on the PCI-card in a way that a set of diodes including for instance three diodes 412, 414, 416 is directed perpendicularly towards the reflective layer 430. The set of diodes 412, 414, 416 is placed on the IR-unit 410 in a row, preferably with an IR-LED (infrared light emitting diode) 416 in the middle and one detecting photodiode 412, 414 on each side of the middle positioned IR-LED 416. Each of the diodes 412, 414, 416 has a non-transparent screening around it in order not to disturb or interfere with the other two diodes. This might occur in that undesired emission that has not been reflected from the reflective layer 430 or other undesired kinds of reflection, such as varying ambient light, would be captured by the detecting photodiodes 412, 414 instead of the properly reflected IR-light which is to be analysed.

The set of diodes 412, 414, 416 is arranged in a way that part of an emitted area and a detected area of the reflective layer will be overlapping. Two of these areas have been illustrated in Fig 1 and have been designated 450 and 452. The intensity of the reflected light energy of these areas 450, 452 is captured by the IR-unit 410 and measurement data on this reflected IR-light intensity is communicated to the micro-controller 100. A certain change in measurement value of the reflected IR-light intensity is a relevant indication that the casing of the computer has been moved, possibly for opening of the casing. Thus the micro-controller 100 is notified about the certain charge and is able to respond to this relevant indication, perhaps by taking corresponding actions of for example initialising an irreversible destruction of certain components of the computer. Hence, the destruction mechanism will be activated before the casing is completely opened. Slow changes in the measured light energy, due to ambient temperature conditions, are detected and compensated by utilisation of a temperature sensor (not shown) in connection with the micro-controller 100.

Furthermore, and still with reference to Fig 1, a remote accessibility unit 500 is shown, by which unit 500 the safeguarding apparatus can be activated in a number of ways. The remote accessibility unit is connected to the micro-controller 100 via another of its inputs/outputs 150. The apparatus for irreversible destruction of stolen electronic equipment has four differently activated states of operation. To the user of for instance a personal computer, the safeguarding apparatus is either in a locked or unlocked state. The user herself/himself has a possibility of locking and unlocking the safeguarded computer, by means of a pocket-sized remote access transmitter 520, including at least one antenna 526, a RF-module (radio frequency module) 524 and a signal encoder 526, by which remote access transmitter 520 messages are encrypted, modulated and transmitted to the corresponding remote access receiver 540. Here they are received, demodulated and decoded, whereby software controlled by the micro-controller 100 is used for decoding the message. Transmission of data is performed in a standardised way over the air interface and the assigned radio frequency band for the customer products is utilised. The remote access receiver 540 is mounted on the PCI-card just like the other previously described units of the destruction means 200. The remote access receiver 540 also includes at least one antenna 544 and an RF-module 542. Except for the remote access transmitter 520, the antenna 544 of the remote access receiver 540 is the only part of the safeguarding arrangement that is not completely inside the computer casing. The antenna is protected by a cover and is coupled to the electric circuit through a capacitor, to prevent from external corruption of the apparatus, for instance by removing the cover and applying high-voltage to the antenna.

The locking and unlocking feature or the electronic equipment, in this embodiment a computer, is realised by redirecting the power switch to the micro-controller 100 and from there connecting to the motherboard of the computer. The connection between motherboard and micro-controller 100 enables checking whether the computer is connected to the external power source 300. The connection between the power switch and the micro-controller 100 enables turning on and turning off the

computer as well as to prevent powering of the computer, which here means to lock the computer.

For professionals, such as administrators or so-called super users, who are serving the computer or for maintenance reasons, it is possible to disarm the activation of the destruction mechanism prior to opening the casing of the computer to prevent undesired destruction of components. Subsequently, i.e. after having carried out technical services, replaced or updated components of the computer, the professional arms the destruction mechanism, whereby the computer is ready for use again. The various states armed/disarmed and locked/unlocked give rise to four different operational states of the computer, of which an ordinary user only accesses the lock and unlock features. Deactivation of the destruction functionality accessible exclusively for professionals, the mentioned administrators and super users.

Another main unit controlled by the micro-controller 100, via the input/output 160, is the user information unit 600. This unit visualises and notifies the user of the safeguarding apparatus about the present state of operation, i.e. armed/disarmed and locked/unlocked state. The user information unit 600 comprises a buzzer 610 for audio signals and at least one diode 620, 622, 624, preferably an LED, emitting visible light. Its is feasible to use visible LEDs of different visible colours and buzzer signals of different frequencies and volume for easy and unambiguous recognition of signal message, also by non-professional users with little technical interest and/or experience. Some of these diodes may be visible from the outside of the computer casing and others only from the inside. Hidden diodes inside the computer casing are to inform professionals when serving or maintaining the electronic equipment.

By means of the safeguarding apparatus of the present invention, a wide variety of components can be irreversibly destructed. In a first embodiment of the invention, destruction of components is obtained by means of transferring a built-up voltage from the loaded capacitor arrangement 220 via the target component switch 225. In

most cases, the rather low level of voltage is applied, approximately as low voltage as 20-40 V, in the opposite direction relative to the usual voltage direction when a component is in a normal state of operation. By applying the voltage in the opposite direction, a rectifier or another type of diode may be broken, whereby the component to be destructed is easily accessible. Some of the valuable components of the computer that can be irreversibly destructed by means of the apparatus are the following: non-volatile memory locations like the hard disk 701 and other disks 702, the motherboard 703 and the central processing unit 704. Also various expansion cards 705 like the graphic card, video card, audio card and network card can be destructed. Other units that are included among components to be destructed are the DVD- 706 and/or CD player 707. In addition to the previously mentioned components, also read only memories 708, flash memories 709, etc, are included. Each valuable and theft-attractive component is safeguarded and can be destructed by means of the apparatus according to the present invention.

A delicate task, which is of crucial importance in a safeguarding apparatus like the present invention, is to prevent undesired destruction of computer components due to unexpected or unwanted events taking place. A single error in a logical signal could, in a worst case scenario, lead to irreversible destruction of all electronic components in a computer. Logical signal errors may occur in all kinds of electronic equipment, so the consequences must not be of the previously mentioned critical nature. The present invention solves the problem in two ways. The voltage used for destruction is generated by a circuitry including a transformer, a rectifier and a load capacitor. Generation of a relatively low level of voltage, which still is sufficient for destruction of components 701-709, can be accomplished by the voltage generating means 215 in a short period of time in comparison to high-voltage levels. According to measurements only a period of a few tenths of a second is required for reaching a voltage level in the capacitor arrangement 220 of about 30 V. Loading of the capacitor arrangement 220 is initiated first when the micro-controller 100 decides to take actions for destruction of components. However, the alternating input voltage is

not generated in usual manners by a distinct oscillating circuit, but by means of the micro-controller 100. The alternating output voltage is produced on one of the output pins of the micro-controller 100 and thus, the alternating output voltage is controlled by software. An erroneous logical signal can not trigger the destruction mechanism of the destruction means 200 unless the required voltage level of the capacitor arrangement 220 has been generated at first. If the either hardware or software of the micro-controller 100 for whatever reason would fail, no alternating signal is produced and hence no voltage will be built-up. Therefore, the destruction mechanism is intrinsically safe and will not ever be activated by mistake.

Another additional safety arrangement, which is achieved by the circuitry design, is that the activation of the destructive capacitor arrangement voltage is performed by the micro-controller 100. This means that even if a voltage has been built-up and is about to be lead on to destruction of electronic components, it does not have to be switched out to the components 701-709 via the target component switch 225. This switching is controlled and performed by the micro-controller 100, whereby activation by mistake will not ever occur in case voltage for destruction already has been built up.

Although the shifts between operational states of the safeguarding apparatus in a first embodiment are made by means of the previously described encoding radio frequency key 520, there are many other conceivable methods for identification and authentication of users. Another way of shifting between operational states, such as unlocking and disarming, is by means of identification procedures, such as using a smart card or manual keying of a PIN-code by an operator or user. When identification is accomplished, the operator or user candidate is compared with a register of predefined authorised operators or users and the candidate may subsequently be authorised for usage of safeguarded electronic equipment. The identification process could also take advantage of any other unique human features and it is conceivable to utilise fingerprint recognition or iris detection techniques.

Moreover, to the function of the destruction means 200, the voltage generating means 215 generates one for the electric circuitry excessively high voltage and/or current, which passes the target component switch 225, and is lead through the circuitry. Preferably it is lead as a reverse current through a diode, whereby essential electronic devices either melt or are otherwise irreversibly damaged and made useless. In another embodiment, destructive highly conductive or corrosive chemical fluid is stored in the vicinity of sensitive the electronic components. At absolute and definite control from the micro-controller 100, the fluid may be set free and can thus be distributed over essential and vulnerable components 701-709 to be safeguarded, and eventually destructed, in the computer. Hereby is achieved a similar way of destruction of essential components either through short-circuiting electrical circuitry or corroding vital components instead of melting as in the first embodiment. Also a combination of the above-mentioned techniques is a feasible and effective way, in which the safeguarding apparatus works.

Except for the locking and unlocking radio frequency key, called the remote access transmitter 520, it is possible to use other wireless interfaced transceiver means. Such means could be a mobile telephone, a PDA and/or a variety of infrared communication terminals, each one of them enabling a way of remote accessibility to the safeguarding apparatus as well as authenticating and identifying the operator or user of the safeguarding apparatus.

Next reference is to Fig 2, which is a flow chart sequentially showing the steps for irreversible destruction of electronic components contained in the computer. Depending on the access rights of the current user or professional, the here used terms activate and inactivate should be changed to lock and unlock. The sequence starts (step 900) with a choice of whether the destruction means 200 is activated (step 901) or not. In case it is not activated, the sequence proceeds with the user's option to activate (step 902) the destruction means 200. If the user decides not to activate it, the sequence ends (step 915), otherwise the destruction means 200 is activated (step 903). In response to this activation, the user information unit 600 indicates

(904) the change in operational state to the user. In case the destruction means already was activated, or currently has become, the sequence follows up with an ongoing analysis (step 905) of the signals transmitted from the sensor means 400. Either, the sensor means 400 is polled by the micro-controller 100, or the sensor means 400 continuously updates the micro-controller 100 about current measurement data. As soon as the computer casing is opened (step 906), the micro-controller 100 is notified about it and has the responsibility for taking further action in response to the indication. As long as the computer casing remains closed, the user has an option to inactivate (step 907) the destruction means 200, for example by locking it. If the user decides to, the destruction means 200 is inactivated (step 908) and proceeds to the end (step 915) of the sequence, otherwise the micro-controller 100 instructs comprised units to continue analysing (step 905) the sensor signals received.

However, if an opening (step 906) of the computer casing is unambiguously detected by the micro-controller 100 and hence a destructive action is to be taken, the micro-controller 100 finds out whether the capacitor arrangement 220 is sufficiently charged (step 909) for enabling the destruction of components. In case it is not, the micro-controller 100 instructs the voltage generating means 215 to charge (step 910) the capacitor arrangement 220 until it has reached a sufficient level of charge. As soon as the sufficient level of charge is reached, the micro-controller 100 instructs the destruction means to destruct (step 911) a first component. As long as any component remains functional (step 912), or has not yet been completely and irreversibly destructed, the target component switch 225 of the destruction means 200 switches (step 913) the focus of destruction to another target component to destruct. When there is no more functional component remaining, the user information unit 600 informs the user about this by indicating (step 914) the destructed state of operation. Hence, the sequence has reached its end (step 915).